Practitioner's Docket No. NAI1P014/01.128.01 *PATENT*

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of: Barton et al.

Application No.: 09/916,929 Group No.: 2137
Filed: 07/26/2001 Examiner: Schubert, K.
For: ANTI-VIRUS SCANNING CO-PROCESSOR

Mail Stop Appeal Briefs – Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

TRANSMITTAL OF APPEAL BRIEF
(PATENT APPLICATION--37 C.F.R. § 41.37)

1. This brief is in furtherance of the Notice of Appeal, filed in this case on 08/01/2006.

2. STATUS OF APPLICANT

This application is on behalf of other than a small entity.

3. FEE FOR FILING APPEAL BRIEF

Pursuant to 37 C.F.R. §1.17(c), the fee for filing the Appeal Brief has already been paid. However, the Commissioner is authorized to charge any fees that may be due to deposit account 50-1351 (NAI1P014).

4. EXTENSION OF TERM

The proceedings herein are for a patent application and the provisions of 37 C.F.R. § 1.136 apply.

Applicant hereby petitions for a Three Month Extension of Time.

Applicant believes that no additional extension of time is necessary however if the examiner feels that fees are due in accordance with the filing of this paper, the examiner is authorized to charge such fees to deposit account 50-1351 order no. (NAI1P014).

5. TOTAL FEE DUE

The total fee due is:

Appeal brief fee	$0.00 (previously paid on December 12, 2005)
Extension of Time Fee	$1020.00
Total Fee Due	$1020.00

6. FEE PAYMENT

Applicant believes that only the above fees are due in connection with the filing of this paper because the appeal brief fee was paid with a previous omission. However, the Commissioner is authorized to charge any additional fees that may be due (e.g. for any reason including, but not limited to fee changes, etc.) to deposit account 50-1351 (Order No. NAI1P014).

7. FEE DEFICIENCY

If any additional extension and/or fee is required, and if any additional fee for claims is required, charge Deposit Account No. 50-1351 (Order No. NAI1P014).

/KEVINZILKA/

Signature of Practitioner

Reg. No.: 41,429
Tel. No.: 408-971-2573
Customer No.: 28875

Kevin J. Zilka
Zilka-Kotab, PC
P.O. Box 721120
San Jose, CA 95172
USA

PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of:	
Barton et al.	Group Art Unit: 2137
Application No. 09/916,929	Examiner: Schubert, Kevin R.
Filed: 07/26/2001	Date: January 3, 2007
For: ANTI-VIRUS SCANNING CO-PROCESSOR	

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

ATTENTION: Board of Patent Appeals and Interferences

APPEAL BRIEF (37 C.F.R. § 41.37)

This brief is in furtherance of the Notice of Appeal, filed in this case on 08/01/2006.

The fees required under § 1.17, and any required petition for extension of time for filing this brief and fees therefor, are dealt with in the accompanying TRANSMITTAL OF APPEAL BRIEF.

This brief contains these items under the following headings, and in the order set forth below (37 C.F.R. § 41.37(c)(i)):

I REAL PARTY IN INTEREST
II RELATED APPEALS AND INTERFERENCES
III STATUS OF CLAIMS
IV STATUS OF AMENDMENTS
V SUMMARY OF CLAIMED SUBJECT MATTER
VI GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

VII ARGUMENT

VIII CLAIMS APPENDIX

IX EVIDENCE APPENDIX

X RELATED PROCEEDING APPENDIX

The final page of this brief bears the practitioner's signature.

I REAL PARTY IN INTEREST (37 C.F.R. § 41.37(c)(1)(i))

The real party in interest in this appeal is McAfee, Inc.

II RELATED APPEALS AND INTERFERENCES (37 C.F.R. § 41.37(c) (1)(ii))

With respect to other prior or pending appeals, interferences, or related judicial proceedings that will directly affect, or be directly affected by, or have a bearing on the Board's decision in the pending appeal, an appeal noted on 06/02/2005 in application serial number 09/916,600 may be, but is not necessarily, related.

Since no decision(s) has been rendered in such proceeding(s), no Related Proceedings Appendix is appended hereto.

III STATUS OF CLAIMS (37 C.F.R. § 41.37(c) (1)(iii))

A. TOTAL NUMBER OF CLAIMS IN APPLICATION

Claims in the application are: 1-13, 17-29 and 33-44

B. STATUS OF ALL THE CLAIMS IN APPLICATION

1. Claims withdrawn from consideration: None
2. Claims pending: 1-13, 17-29 and 33-44
3. Claims allowed: None
4. Claims rejected: 1-13, 17-29 and 33-44
5. Claims cancelled: 14-16, and 30-32

C. CLAIMS ON APPEAL

The claims on appeal are: 1-13, 17-29 and 33-44

See additional status information in the Appendix of Claims.

IV STATUS OF AMENDMENTS (37 C.F.R. § 41.37(c)(1)(iv))

As to the status of any amendment filed subsequent to final rejection, there are no such amendments after final.

V SUMMARY OF CLAIMED SUBJECT MATTER (37 C.F.R. § 41.37(c)(1)(v))

With respect to a summary of Claim 1, as shown in Figures 5 and 6, a technique is provided for scanning data. In use, scanning control logic is executed utilizing a central processing unit (e.g. item 502 of Figure 5) and the data is indicated to a scanning co-processor coupled to the central processing unit so that the data is scanned by the scanning co-processor under the control of the scanning control logic (e.g. item 510/514 of Figure 5). Results from the scanning co-processor are waited for (e.g. decision 516 of Figure 5) and additional logic is executed utilizing the central processing unit while waiting for the results from the scanning co-processor (e.g. item 514 of Figure 5). In addition, an event is initiated based on the results from the scanning co-processor (e.g. item 518 of Figure 5). The scanning co-processor is also under the control of the central processing unit via the execution of the scanning control logic by the central processing unit. Furthermore, it is determined whether the data meets a predetermined criteria, where the criteria is based on a type of a file associated with the data (e.g. item 506 of Figure 5) and the data is sent to the scanning co-processor if it is determined that the data meets the predetermined criteria (e.g. operation 508 of Figure 5). Still yet, additional data to be scanned by the scanning co-processor is queued while waiting for the results from the scanning co-processor (e.g. item 610 of Figure 6). Note page 3, line 1-page 4, line 4, for example.

With respect to a summary of Claim 17, as shown in Figures 5 and 6, a computer program product for scanning data comprises computer code for executing scanning control logic utilizing a central processing unit (e.g. item 502 of Figure 5), and a request related to data is identified at the central processing unit. In addition, the data is indicated to a scanning co-processor coupled to the central processing unit so that the data is scanned by the scanning co-processor under the control of the scanning control logic (e.g. item 510/514 of Figure 5). Additionally, results from the scanning co-processor are waited for (e.g. item 516 of Figure 5) and additional logic is executed utilizing the central processing unit while waiting for the results from the scanning co-processor (e.g. item 514 of Figure 5). Further, an event is initiated based on the results from the scanning co-processor (e.g. item 518 of Figure 5). The scanning co-processor is under the control of the central processing unit via the execution of the scanning control logic by the central processing unit. Also, it is determined whether the data meets a predetermined criteria,

where the criteria is based on a type of a file associated with the data (e.g. item 506 of Figure 5), and the data is sent to the scanning co-processor if it is determined that the data meets the predetermined criteria (e.g. item 508 of Figure 5). Further, additional data to be scanned by the scanning co-processor is queued while waiting for the results from the scanning co-processor (e.g. item 610 of Figure 6). Note page 3, line 1-page 4, line 4, for example.

With respect to a summary of Claim 33, as shown in Figures 5 and 6, a system for scanning data, comprises logic for executing scanning control logic utilizing a central processing unit (e.g. item 502 of Figure 5), and logic for identifying a request related to data at the central processing unit. In addition, the system comprises logic for indicating the data to a scanning co-processor coupled to the central processing unit so that the data is scanned by the scanning co-processor under the control of the scanning control logic (e.g. item 510/514 of Figure 5). Additionally, the system comprises logic for waiting for results from the scanning co-processor (e.g. item 516 of Figure 5), and logic for executing additional logic utilizing the central processing unit while waiting for the results from the scanning co-processor (e.g. item 514 of Figure 5). Also, the system comprises logic for initiating an event based on the results from the scanning co-processor (e.g. item 518 of Figure 5). The scanning co-processor is under the control of the central processing unit via the execution of the scanning control logic by the central processing unit. Also, it is determined whether the data meets a predetermined criteria, where the criteria is based on a type of a file associated with the data (e.g. item 506 of Figure 5), and the data is sent to the scanning co-processor if it is determined that the data meets the predetermined criteria (e.g. item 508 of Figure 5). Further, additional data to be scanned by the scanning co-processor is queued while waiting for the results from the scanning co-processor (e g. item 610 of Figure 6). Note page 3, line 1-page 4, line 4, for example.

With respect to a summary of Claim 34, as shown in Figures 5 and 6, a method for scanning data comprises executing scanning control logic utilizing a central processing unit (e.g. item 502 of Figure 5) and a request related to data is identified at the central processing unit. In addition, it is determining whether the data meets a predetermined criteria utilizing the central processing unit under the control of the scanning control logic (e.g. item 510/514 of Figure 5). Additionally, the data is indicated to a scanning co-processor coupled to the central processing unit if it is determined that the data meets the predetermined criteria (e.g. item 508 of Figure 5).

Furthermore, scanning information is collected from memory on the scanning co-processor (e.g. item 602 of Figure 6), and the data is scanned with the scanning co-processor utilizing the scanning information under the control of the scanning control logic (e.g. item 604 of Figure 6). In addition, results from the scanning co-processor are waited for (e.g. item 516 of Figure 5), and additional logic is executed utilizing the central processing unit while waiting for the results from the scanning co-processor (e.g. item 514 of Figure 5). Further, additional data to be scanned is queued by the scanning co-processor while waiting for the results from the scanning co-processor (e.g. item 610 of Figure 6). In addition, a security event is initiated upon the receipt of unfavorable results from the scanning co-processor including a situation where malicious code is detected (e.g. item 518 of Figure 5). Additionally, the data is processed utilizing the central processing unit upon the receipt of favorable results from the scanning co-processor including a situation where malicious code is not detected (e.g. item 520 of Figure 5). Also, the scanning co-processor is under the control of the central processing unit via the execution of the scanning control logic by the central processing unit. Furthermore, the criteria is based on a type of a file associated with the data. Note page 3, line 1-page 4, line 4; and page 11, lines 4-9, for example.

With respect to a summary of Claim 35, as shown in Figures 5 and 6, a system for scanning data comprises means for executing scanning control logic utilizing a central processing unit (e.g. item 502 of Figure 5). In addition, the system comprises means for identifying a request related to data at the central processing unit (e.g. item 504 of Figure 5). Further, the system comprises means for determining whether the data meets a predetermined criteria utilizing the central processing unit under the control of the scanning control logic (e.g. item 506 of Figure 5). Additionally, the system comprises means for indicating the data to a scanning co-processor coupled to the central processing unit if it is determined that the data meets the predetermined criteria (e.g. item 508 of Figure 5). Furthermore, the system comprises means for collecting scanning information from memory on the scanning co-processor (e.g. item 602 of Figure 6). In addition, the system comprises means for scanning the data with the scanning co-processor utilizing the scanning information under the control of the scanning control logic (e.g. item 604 of Figure 6). Further, the system comprises means for waiting for results from the scanning co-processor (e.g. item 516 of Figure 5). Still yet, the system comprises means for executing additional logic utilizing the central processing unit while waiting for the results from the scanning co-processor (e.g. item 514 of Figure 5). In addition, the system comprises means for

queuing additional data to be scanned by the scanning co-processor while waiting for the results from the scanning co-processor (e.g. item 610 of Figure 6). Furthermore, the system comprises means for initiating a security event upon the receipt of unfavorable results from the scanning co-processor including a situation where malicious code is detected (e.g. item 518 of Figure 5). Also, the system comprises means for processing the data utilizing the central processing unit upon the receipt of favorable results from the scanning co-processor including a situation where malicious code is not detected (e.g. item 520 of Figure 5). The scanning co-processor is under the control of the central processing unit via the execution of the scanning control logic by the central processing unit. Further, the criteria is based on a type of a file associated with the data. Note page 3, line 1-page 4, line 4, for example.

VI GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL (37 C.F.R. § 41.37(c)(1)(vi))

Following, under each issue listed, is a concise statement setting forth the corresponding ground of rejection.

Issue #1: The Examiner has rejected Claims 2, 18, and 34-37 under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which appellant regards as the invention.

Issue #2: The Examiner has rejected Claims 1-2, 4-13, 17-18, 20-29, 33-35, 38-40, 42 and 44 under 35 U.S.C. 102(e) as being anticipated by Grupe et al. (U.S. Publication No. 2002/0194212).

Issue #3: The Examiner has rejected Claims 3, 19, 36, 41 and 43 under 35 U.S.C. 103(a) as being unpatentable over Grupe et al. (U.S. Publication No. 2002/0194212), in view of Zuta (International Publication No. WO 98/45778).

Issue #4: The Examiner has rejected Claim 37 under 35 U.S.C. 103(a) as being unpatentable over Grupe et al. (U.S. Publication No. 2002/0194212), in view of Snavely (Snavely, Allan; Tullsen, Dean. Symbiotic Jobscheduling for a Simultaneous Multithreading Processor. Published in the Proceedings of ASPLOS IX. November 2000).

VII ARGUMENT (37 C.F.R. § 41.37(c)(1)(vii))

The claims of the groups noted below do not stand or fall together. In the present section, appellant explains why the claims of each group are believed to be separately patentable.

Issue #1:

The Examiner has rejected Claims 2, 18, and 34-37 under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which appellant regards as the invention. Appellant respectfully disagrees with the Examiner's rejection. Specifically, the Examiner argued that there is no definitive standard for ascertaining what constitutes "favorable results" and "unfavorable results." However, appellant respectfully asserts that appellant claims "unfavorable results" as "including a situation where malicious code is detected" (emphasis added) and "favorable results" as "including a situation where malicious code is not detected (emphasis added), as claimed. Clearly, appellant's claimed techniques set the standards for "favorable results" and "unfavorable results."

Issue #2:

The Examiner has rejected Claims 1-2, 4-13, 17-18, 20-29, 33-35, 38-40, 42 and 44 under 35 U.S.C. 102(e) as being anticipated by Grupe et al. (U.S. Publication No. 2002/0194212).

Group #1: Claims 1, 4-7, 9-11, 13, 17, 20-23, 25-27, 29, 33, 40, and 42

he Examiner has relied on Paragraphs 0008, and 0009 from Grupe to meet appellant's claimed technique "wherein the scanning co-processor is under the control of the central processing unit via the execution of the scanning control logic by the central processing unit" (see this or similar, but not necessarily identical language in the independent Claims 1, 17, and 33).

> "Viewed from one aspect the present invention provides a computer program product comprising **a computer program operable to control a scanning computer to produce a log file identifying computer data from a source computer having specified content,** said computer program comprising: scanning logic operable to scan computer data transferred from said source computer to said scanning computer and to identify one

> or more portions of said computer data having one or more predetermined characteristics indicative of said computer data having said specified content; and log generating logic operable to write details of said identified portions to a log file.
>
> The invention recognises the above problem of scans of computer data that take so long that a complete scan of the data cannot be performed during slack time, such as overnight or during the weekend. **To address this problem embodiments of the invention transfer data to be scanned from a source computer to a scanning computer. The scanning computer then scans the data and creates a log file identifying portions of the data that have predetermined characteristics indicating a particular specified content.** This enables the source computer to rescan or otherwise selectively process the data identified in the log file, which considerably reduces the processing time of the source computer needed for a scan." (Paragraphs 0008-0009 - emphasis added)

Appellant respectfully asserts that the excerpts from Grupe relied upon by the Examiner merely disclose "a computer program operable to control a scanning computer to produce a log file identifying computer data from a source computer having specified content." Further, Grupe discloses that "data to be scanned [is transferred] from a source computer to a scanning computer" where "[t]he scanning computer then scans the data and creates a log file identifying portions of the data that have predetermined characteristics indicating a particular specified content" (emphasis added). However, the mere disclosure of transferring data from a source computer to a scanning computer, where the scanning computer scans the data and creates a log file, as in Grupe, fails to even suggest a technique "wherein the scanning co-processor is under the control of the central processing unit via the execution of the scanning control logic by the central processing unit" (emphasis added), as claimed by appellant. Clearly, since the scanning computer disclosed by Grupe is not under the control of the source computer, then Grupe fails to disclose "wherein the scanning co-processor is under the control of the central processing unit via the execution of the scanning control logic by the central processing unit" (emphasis added), as claimed by appellant.

Furthermore, the Examiner has relied on Paragraph 0009 from Grupe to make a prior art showing of appellant's claimed technique "wherein additional data to be scanned by the scanning co-processor is queued while waiting for the results from the scanning co-processor" (see this or similar, but not necessarily identical language in the independent Claims 1, 17, and 33).

> "The invention recognises the above problem of scans of computer data that take so long that a complete scan of the data cannot be performed

during slack time, such as overnight or during the weekend. To address **this problem embodiments of the invention transfer data to be scanned from a source computer to a scanning computer. The scanning computer then scans the data and creates a log file identifying portions of the data that have predetermined characteristics indicating a particular specified content.** This enables the source computer to rescan or otherwise selectively process the data identified in the log file, which considerably reduces the processing time of the source computer needed for a scan." (Paragraph 0009 - emphasis added)

Appellant respectfully asserts that the excerpt from Grupe relied upon by the Examiner merely discloses that "data to be scanned [is transferred] from a source computer to a scanning computer" where "[t]he scanning computer **then** scans the data and creates a log file identifying portions of the data that have predetermined characteristics indicating a particular specified content" (emphasis added). However, the mere disclosure that the data to be scanned is transferred to the scanning computer where the scanning computer then scans the data and creates a log file, as in Grupe, fails to even suggest a technique "wherein additional data to be scanned by the scanning co-processor is queued **while** waiting for the results from the scanning co-processor" (emphasis added), as claimed by appellant. Clearly, transferring the data to be scanned and then scanning the data, as in Grupe, fails to suggest "[queuing] additional data to be scanned... **while** waiting for the results from the scanning co-processor" (emphasis added), as claimed by appellant.

The Examiner is reminded that a claim is anticipated only if each and every element as set forth in the claim is found, either expressly or inherently described in a single prior art reference. *Verdegaal Bros. v. Union Oil Co. Of California*, 814 F.2d 628, 631, 2 USPQ2d 1051, 1053 (Fed. Cir. 1987). Moreover, the identical invention must be shown in as complete detail as contained in the claim. *Richardson v. Suzuki Motor Co.*868 F.2d 1226, 1236, 9USPQ2d 1913, 1920 (Fed. Cir. 1989). The elements must be arranged as required by the claim.

This criterion has simply not been met by the Grupe reference, especially in view of the arguments made hereinabove.

Group #2: Claims 2 and 18

The Examiner has relied on Paragraph 0015 from Grupe to make a prior art showing of appellant's claimed "processing the data utilizing the central processing unit upon the receipt of favorable results from the scanning co-processor including a situation where malicious code is not detected."

> "A further aspect of the present invention provides a computer program product comprising a computer program operable to control a source computer to scan computer data stored by said source computer to identify one or more portions of said computer data having one or more predetermined characteristics indicative of said computer data having some specified content, said computer program comprising: **log reading logic operable to control said source computer to read a log file written by a scanning computer, said log file identifying portions of said computer data having said predetermined characteristics; and response logic responsive to said log file and operable to control said source computer to perform further processing tasks upon at least said data identified in said log file as having said predetermined characteristics.**" (Paragraph 0015 - emphasis added)

Appellant respectfully asserts that the excerpt from Grupe relied upon by the Examiner merely discloses that "log reading logic [is] operable to control said source computer to read a log file written by a scanning computer [where] said log file identifies] portions of said computer data having said predetermined characteristics" (emphasis added). Further, Grupe discloses that "said source computer ... perform[s] further processing tasks upon at least said data identified in said log file as having said predetermined characteristics" (emphasis added). However, the mere disclosure of performing further processing tasks upon a log file which identifies portions of computer data having predetermined characteristics, as in Grupe, fails to even suggest "processing the data utilizing the central processing unit upon the receipt of favorable results from the scanning co-processor including a situation where malicious code is **not** detected" (emphasis added), as claimed by appellant.

In the Office Action mailed 05/01/2006, the Examiner argued that "the log file allows the user to ascertain which data is malicious (needing re-scanning)" and "[t]he other data is clean." Appellant respectfully disagrees and asserts that Grupe merely discloses that "said log file identifies] portions of said computer data having said predetermined characteristics" (emphasis added). Clearly, identifying portions of computer data having predetermined characteristics, as in Grupe, fails to even suggest "the receipt of favorable results from the scanning co-processor

including a situation where malicious code is **not** detected" (emphasis added), as claimed by appellant.

Further, the Examiner argued that there is no definitive standard for ascertaining what constitutes "favorable results" and "unfavorable results." However, appellant respectfully asserts that appellant claims "unfavorable results" as "including a situation where malicious code is detected" (emphasis added) and "favorable results" as "including a situation where malicious code is not detected (emphasis added). Clearly, appellant's claimed techniques set the standards for "favorable results" and "unfavorable results."

Again, appellant respectfully asserts that appellant's specific claim language is not anticipated by the Grupe reference since all of appellant's claim limitations have not been met by the Grupe reference, as noted above.

Group #3: Claims 8 and 24

The Examiner has relied on Paragraphs 0010 and 0011 in Grupe to make a prior art showing of appellant's claimed technique "wherein the event is initiated under the control of the scanning control logic."

> "Although the log file may be transferred back to the source computer by the use of tapes or disks, **it is preferable that the computer program product comprises log transferring logic operable to control said scanning computer to transfer said log file, via a network connection to said source computer.**
>
> Although any content of data that the user cares to specify may be scanned for, embodiments of the invention are particularly well suited to scanning for one or more of: a computer virus; a worm; a Trojan; and a computer file comprising banned content. Alternatively, embodiments of the invention can be used as part of an e-mail or file storage filtering system, wherein the specified content includes banned words or phrases." (Paragraphs 0010-0011 – emphasis added)

Appellant respectfully asserts that "log transferring logic [is] operable to control said scanning computer to transfer said log file, via a network connection to said source computer" (emphasis added). However, the mere disclosure that log transferring logic transfers the log file from the scanning computer to the source computer fails to even suggest a technique "wherein the event is

initiated under the control of the scanning control logic" (emphasis added), as claimed by appellant.

Again, appellant respectfully asserts that appellant's specific claim language is not anticipated by the Grupe reference since all of appellant's claim limitations have not been met by the Grupe reference, as noted above.

Group #4: Claims 12 and 28

The Examiner has relied on Paragraphs 0011 and 0028 in Grupe to make a prior art showing of appellant's claimed technique "wherein virus signatures are stored in the memory."

> "Although any content of data that the user cares to specify may be scanned for, embodiments of the invention are particularly well suited to scanning for one or more of: a computer virus; a worm; a Trojan; and a computer file comprising banned content. Alternatively, embodiments of the invention can be used as part of an e-mail or file storage filtering system, wherein the specified content includes banned words or phrases." (Paragraph 0011)

> "In operation the network storage device 18 is subject to regular on-demand scans to identify computer viruses, Trojans, Worms and/or files with banned content. **As the network storage device 18 can be very large, the amount of processing time required to compare every stored file against an increasing number of virus definition profiles can be extremely long.** In general, the server 4 performs such scans during quiet times, such as the night or weekend. Given the increasing length of time required for such scans, it may well be that it is not possible to complete these scans during the quiet times. This could result in incomplete scans which carry the risk of viruses going undetected. " (Paragraph 0028 – emphasis added)

Appellant respectfully asserts that the excerpts from Grupe relied upon by the Examiner merely disclose that "[a]s the network storage device 18 can be very large, the amount of processing time required to compare every **stored file** against an increasing number of virus definition profiles can be extremely long" (emphasis added). However, the mere disclosure in Grupe that the stored files are compared against an increasing number of virus definition profiles fails to teach a technique "wherein virus signatures are stored in the memory" (emphasis added), as claimed by appellant.

Again, appellant respectfully asserts that appellant's specific claim language is not anticipated by the Grupe reference since all of appellant's claim limitations have not been met by the Grupe reference, as noted above.

Group #5: Claims 34 and 35

Furthermore, the Examiner has relied on Paragraph 0009 from Grupe to make a prior art showing of appellant's claimed "queuing additional data to be scanned by the scanning co-processor while waiting for the results from the scanning co-processor" (see this or similar, but not necessarily identical language in the independent Claims 34 and 35).

> "The invention recognises the above problem of scans of computer data that take so long that a complete scan of the data cannot be performed during slack time, such as overnight or during the weekend. To address **this problem embodiments of the invention transfer data to be scanned from a source computer to a scanning computer. The scanning computer then scans the data and creates a log file identifying portions of the data that have predetermined characteristics indicating a particular specified content.** This enables the source computer to rescan or otherwise selectively process the data identified in the log file, which considerably reduces the processing time of the source computer needed for a scan." (Paragraph 0009 – emphasis added)

Appellant respectfully asserts that the excerpt from Grupe relied upon by the Examiner merely discloses that "data to be scanned [is transferred] from a source computer to a scanning computer" where "[t]he scanning computer **then** scans the data and creates a log file identifying portions of the data that have predetermined characteristics indicating a particular specified content" (emphasis added). However, the mere disclosure in Grupe that the data to be scanned is transferred to the scanning computer where the scanning computer then scans the data and creates a log file fails to even suggest "queuing additional data to be scanned by the scanning co-processor **while** waiting for the results from the scanning co-processor" (emphasis added), as claimed by appellant. Clearly, transferring the data to be scanned and then scanning the data, as in Grupe, fails to suggest "queuing additional data to be scanned **while** waiting for the results from the scanning co-processor" (emphasis added), as claimed by appellant.

Further, the Examiner has relied on Paragraph 0015 from Grupe to make a prior art showing of appellant's claimed "processing the data utilizing the central processing unit upon the receipt of

favorable results from the scanning co-processor including a situation where malicious code is not detected" (see this or similar, but not necessarily identical language in the independent Claims 34 and 35).

> "A further aspect of the present invention provides a computer program product comprising a computer program operable to control a source computer to scan computer data stored by said source computer to identify one or more portions of said computer data having one or more predetermined characteristics indicative of said computer data having some specified content, said computer program comprising: **log reading logic operable to control said source computer to read a log file written by a scanning computer, said log file identifying portions of said computer data having said predetermined characteristics; and response logic responsive to said log file and operable to control said source computer to perform further processing tasks upon at least said data identified in said log file as having said predetermined characteristics.**" (Paragraph 0015 - emphasis added)

Appellant respectfully asserts that the excerpt from Grupe relied upon by the Examiner merely discloses that "log reading logic [is] operable to control said source computer to read a log file written by a scanning computer [where] said log file identifies] portions of said computer data having said predetermined characteristics" (emphasis added). Further, Grupe discloses that "said source computer ... perform[s] further processing tasks upon at least said data identified in said log file as having said predetermined characteristics" (emphasis added). However, the mere disclosure of performing further processing tasks upon a log file which identifies portions of computer data having predetermined characteristics, as in Grupe, fails to even suggest "processing the data utilizing the central processing unit upon the receipt of favorable results from the scanning co-processor including a situation where malicious code is **not** detected" (emphasis added), as claimed by appellant.

In the Office Action mailed 05/01/2006, the Examiner argued that "the log file allows the user to ascertain which data is malicious (needing re-scanning)" and "[t]he other data is clean." Appellant respectfully disagrees and asserts that Grupe merely discloses that "said log file identifies] portions of said computer data having said predetermined characteristics" (emphasis added). Clearly, identifying portions of computer data having predetermined characteristics fails to even suggest "the receipt of favorable results from the scanning co-processor including a situation where malicious code is **not** detected" (emphasis added), as claimed by appellant.

Again, appellant respectfully asserts that appellant's specific claim language is not anticipated by the Grupe reference since all of appellant's claim limitations have not been met by the Grupe reference, as noted above.

Group #6: Claim 38

The Examiner has relied on Paragraph 0036 in Grupe to make a prior art showing of appellant's claimed technique "wherein the criteria is further based on a user."

> "In the above embodiments the scanning of files is generally done to detect such things as viruses and worms. However, **embodiments of the above invention can be used to detect any content of a file that the user specifies.** Thus, if a system administrator wishes a particular games program to be banned from the system details of the program can be added to the library of data to be scanned for. Alternatively if a check on all e-mail is required in order to confirm, for example, that there is no pornographic material present, then a scan of the stored volume of mail for particular banned words can be made." (Paragraph 0036 - emphasis added)

Appellant respectfully asserts that the excerpt from Grupe relied upon by the Examiner teaches that "embodiments of the above invention can be used to detect any content of a file that the user specifies." However, detecting user specified content of a file, as in Grupe, fails to even suggest a technique "wherein the criteria is further based on a user" (emphasis added), as claimed by appellant.

Again, appellant respectfully asserts that appellant's specific claim language is not anticipated by the Grupe reference since all of appellant's claim limitations have not been met by the Grupe reference, as noted above.

Group #7: Claim 39

The Examiner has relied on Paragraph 0036 in Grupe to make a prior art showing of appellant's claimed technique "wherein the criteria is further based on software logic run by a bios."

> "In the above embodiments the scanning of files is generally done to detect such things as viruses and worms. However, **embodiments of the above invention can be used to detect any content of a file that the**

> **user specifies.** Thus, if a system administrator wishes a particular games program to be banned from the system details of the program can be added to the library of data to be scanned for. Alternatively if a check on all e-mail is required in order to confirm, for example, that there is no pornographic material present, then a scan of the stored volume of mail for particular banned words can be made." (Paragraph 0036 – emphasis added)

Appellant respectfully asserts that the excerpt from Grupe relied upon by the Examiner teaches that "embodiments of the above invention can be used to detect any content of a file that the user specifies." However, detecting user specified content of a file, as in Grupe, fails to even suggest a technique "wherein the criteria is further based on software logic **run** by a bios" (emphasis added), as claimed by appellant.

Again, appellant respectfully asserts that appellant's specific claim language is not anticipated by the Grupe reference since all of appellant's claim limitations have not been met by the Grupe reference, as noted above.

Group #8: Claim 44

The Examiner has relied on Paragraph 0016 in Grupe to make a prior art showing of appellant's claimed technique "wherein the central processing unit aids the scanning co-processor when a large amount of data is to be scanned."

> "In some embodiments of the invention said computer data comprises a fraction of data stored on said source computer, **said computer program product being operable to control said source computer to transmit at least one further fraction of said data to at least one further scanning computer, and to control said source computer to receive a log file from each of said at least one further scanning computers.** By dividing the data to be scanned into different fractions and sending each fraction to a different scanning computer, a scan can be performed in less time that it would take a single scanning computer. Thus, in a situation where it was not possible to do a complete scan during a slack period, such as overnight, on a single computer, it may be possible to perform such a scan on a plurality of computers." (Paragraph 0016 – emphasis added)

Appellant respectfully asserts that the excerpt from Grupe relied upon by the Examiner teaches that "said computer program product being operable to control said source computer to transmit at least one further fraction of said data to at least one further scanning computer, and to control

said source computer to receive a log file from each of said at least one further scanning computers" (emphasis added). However, the mere disclosure that the source computer transmits one further fraction of said data to at least one further scanning computer, as in Grupe, fails to even suggest a technique "wherein the central processing unit **aids** the scanning co-processor when a large amount of data is to be scanned" (emphasis added), as claimed by appellant. Clearly, transmitting a fraction of data to several scanning computers, as in Grupe, fails to suggest that the "the central processing unit aids the scanning co-processor" (emphasis added), in the manner as claimed by appellant.

Again, appellant respectfully asserts that appellant's specific claim language is not anticipated by the Grupe reference since all of appellant's claim limitations have not been met by the Grupe reference, as noted above.

Issue #3:

The Examiner has rejected Claims 3, 19, 36, 41 and 43 under 35 U.S.C. 103(a) as being unpatentable over Grupe et al. (U.S. Publication No. 2002/0194212), in view of Zuta (International Publication No. WO 98/45778).

Group #1: Claims 3, 19, and 43

Appellant respectfully asserts that such claims have not been met by the prior art by virtue of the arguments made in Issue #2, Group #1 above.

Group #2: Claim 36

Appellant respectfully asserts that such claims have not been met by the prior art by virtue of the arguments made in Issue #2, Group #5 above.

Group #3: Claim 41

The Examiner has relied on page 24, lines 1-3 in Zuta to make a prior art showing of appellant's claimed technique "wherein the scanning control logic is executed automatically when a computer is booted up."

> "At power-up the controller 21 loads known viruses pattern as well as sensitive operations which demand further scrutiny, like interrupts or file operations or I/O. The smart verification is detailed below." (Zuta, Page 24, lines 1-3)

Appellant respectfully asserts that such excerpt merely discloses that at power-up "the controller 21 loads known viruses pattern as well as sensitive operations which demand further scrutiny." Clearly, loading a "known viruses pattern" and "sensitive operations which demand further scrutiny" at power-up, as in Zuta, fail to teach a technique "wherein the scanning control logic is executed automatically when a computer is booted up" (emphasis added), as claimed by appellant.

To establish a *prima facie* case of obviousness, three basic criteria must be met. First, there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or to combine reference teachings. Second, there must be a reasonable expectation of success. Finally, the prior art reference (or references when combined) must teach or suggest all the claim limitations. The teaching or suggestion to make the claimed combination and the reasonable expectation of success must both be found in the prior art and not based on appellant's disclosure. *In re Vaeck*, 947 F.2d 488, 20 USPQ2d 1438 (Fed.Cir.1991).

With respect to the first element of the prima facie case of obviousness and, in particular, the obviousness of combining the aforementioned references, the Examiner argued that it would have been obvious to one of ordinary skill in the art at the time of invention to incorporate the ideas of Zuta with those of Grupe and add the use of a bus between the CPU of the first computer and the scanning co-processor of the second computer because a bus is a commonly used method of transmitting data between two units. Appellant respectfully disagrees with such statement, especially in view of the vast evidence to the contrary.

For example, the Examiner fails to cite specific motivation in the above references to support the case for combining the same. The Examiner is reminded that the Federal Circuit requires that there must be some logical reason apparent from the evidence of record that would justify the combination or modification of references. In re Regel, 188 USPQ 132 (CCPA 1975).

Appellant respectfully asserts that at least the first and third element of the *prima facie* case of obviousness have not been met, since it would be *unobvious* to combine the references, as noted above, and the prior art references, when combined, fail to teach or suggest all of the claim limitations, as noted above.

Issue #4:

The Examiner has rejected Claim 37 under 35 U.S.C. 103(a) as being unpatentable over Grupe et al. (U.S. Publication No. 2002/0194212), in view of Snavely (Snavely, Allan; Tullsen, Dean. Symbiotic Jobscheduling for a Simultaneous Multithreading Processor. Published in the Proceedings of ASPLOS IX. November 2000).

Group #1: Claim 37

Appellant respectfully asserts that such claims have not been met by the prior art by virtue of the arguments made in Issue #2, Group #5 above.

In view of the remarks set forth hereinabove, all of the independent claims are deemed allowable, along with any claims depending therefrom.

VIII CLAIMS APPENDIX (37 C.F.R. § 41.37(c)(1)(viii))

The text of the claims involved in the appeal (along with associated status information) is set forth below:

1. (Previously Presented) A method for scanning data, comprising:

a) executing scanning control logic utilizing a central processing unit;

b) identifying a request related to data at the central processing unit;

c) indicating the data to a scanning co-processor coupled to the central processing unit so that the data is scanned by the scanning co-processor under the control of the scanning control logic;

d) waiting for results from the scanning co-processor;

e) executing additional logic utilizing the central processing unit while waiting for the results from the scanning co-processor; and

f) initiating an event based on the results from the scanning co-processor;

wherein the scanning co-processor is under the control of the central processing unit via the execution of the scanning control logic by the central processing unit;

wherein it is determined whether the data meets a predetermined criteria, where the criteria is based on a type of a file associated with the data;

wherein the data is sent to the scanning co-processor if it is determined that the data meets the predetermined criteria;

wherein additional data to be scanned by the scanning co-processor is queued while waiting for the results from the scanning co-processor.

2. (Previously Presented) The method as recited in claim 1, and further comprising processing the data utilizing the central processing unit upon the receipt of favorable results from the scanning co-processor including a situation where malicious code is not detected.

3. (Original) The method as recited in claim 1, wherein the central processing unit is coupled to the scanning co-processor via a bus.

4. (Original) The method as recited in claim 1, wherein the scanning control logic includes hardware.

5. (Original) The method as recited in claim 3, wherein the scanning control logic is stored on the scanning co-processor.

6. (Original) The method as recited in claim 1, wherein the scanning control logic includes software.

7. (Original) The method as recited in claim 6, wherein the scanning control logic is stored in memory.

8. (Original) The method as recited in claim 1, wherein the event is initiated under the control of the scanning control logic.

9. (Original) The method as recited in claim 1, wherein the scanning co-processor performs content scanning.

10. (Original) The method as recited in claim 1, wherein the scanning co-processor performs virus scanning.

11. (Original) The method as recited in claim 1, wherein the scanning co-processor includes memory.

12. (Original) The method as recited in claim 11, wherein virus signatures are stored in the memory.

13. (Original) The method as recited in claim 11, wherein rule sets are stored in the memory.

14. (Cancelled)

15. (Cancelled)

16. (Cancelled)

17. (Previously Presented) A computer program product for scanning data, comprising:

a) computer code for executing scanning control logic utilizing a central processing unit;

b) computer code for identifying a request related to data at the central processing unit;

c) computer code for indicating the data to a scanning co-processor coupled to the central processing unit so that the data is scanned by the scanning co-processor under the control of the scanning control logic;

d) computer code for waiting for results from the scanning co-processor;

e) computer code for executing additional logic utilizing the central processing unit while waiting for the results from the scanning co-processor; and

f) computer code for initiating an event based on the results from the scanning co-processor;

wherein the scanning co-processor is under the control of the central processing unit via the execution of the scanning control logic by the central processing unit;

wherein it is determined whether the data meets a predetermined criteria, where the criteria is based on a type of a file associated with the data;

wherein the data is sent to the scanning co-processor if it is determined that the data meets the predetermined criteria;

wherein additional data to be scanned by the scanning co-processor is queued while waiting for the results from the scanning co-processor.

18. (Previously Presented) The computer program product as recited in claim 17, and further comprising computer code for processing the data utilizing the central processing unit upon the receipt of favorable results from the scanning co-processor including a situation where malicious code is not detected.

19. (Original) The computer program product as recited in claim 17, wherein the central processing unit is coupled to the scanning co-processor via a bus.

20. (Original) The computer program product as recited in claim 17, wherein the scanning control logic includes hardware.

21. (Original) The computer program product as recited in claim 20, wherein the scanning control logic is stored on the scanning co-processor.

22. (Original) The computer program product as recited in claim 17, wherein the scanning control logic includes software.

23. (Original) The computer program product as recited in claim 22, wherein the scanning control logic is stored in memory.

24. (Original) The computer program product as recited in claim 17, wherein the event is initiated under the control of the scanning control logic.

25. (Original) The computer program product as recited in claim 17, wherein the scanning co-processor performs content scanning.

26. (Original) The computer program product as recited in claim 17, wherein the scanning co-processor performs virus scanning.

27. (Original) The computer program product as recited in claim 17, wherein the scanning co-processor includes memory.

28. (Original) The computer program product as recited in claim 27, wherein virus signatures are stored in the memory.

29. (Original) The computer program product as recited in claim 27, wherein rule sets are stored in the memory.

30. (Cancelled)

31. (Cancelled)

32. (Cancelled)

33. (Previously Presented) A system for scanning data, comprising:

a) logic for executing scanning control logic utilizing a central processing unit;

b) logic for identifying a request related to data at the central processing unit;

c) logic for indicating the data to a scanning co-processor coupled to the central processing unit so that the data is scanned by the scanning co-processor under the control of the scanning control logic;

d) logic for waiting for results from the scanning co-processor;

e) logic for executing additional logic utilizing the central processing unit while waiting for the results from the scanning co-processor; and

f) logic for initiating an event based on the results from the scanning co-processor;

wherein the scanning co-processor is under the control of the central processing unit via the execution of the scanning control logic by the central processing unit;

wherein it is determined whether the data meets a predetermined criteria, where the criteria is based on a type of a file associated with the data;

wherein the data is sent to the scanning co-processor if it is determined that the data meets the predetermined criteria;

wherein additional data to be scanned by the scanning co-processor is queued while waiting for the results from the scanning co-processor.

34. (Previously Presented) A method for scanning data, comprising:

a) executing scanning control logic utilizing a central processing unit;

b) identifying a request related to data at the central processing unit;

c) determining whether the data meets a predetermined criteria utilizing the central processing unit under the control of the scanning control logic;

d) indicating the data to a scanning co-processor coupled to the central processing unit if it is determined that the data meets the predetermined criteria;

e) collecting scanning information from memory on the scanning co-processor;

f) scanning the data with the scanning co-processor utilizing the scanning information under the control of the scanning control logic;

g) waiting for results from the scanning co-processor;

h) executing additional logic utilizing the central processing unit while waiting for the results from the scanning co-processor;

i) queuing additional data to be scanned by the scanning co-processor while waiting for the results from the scanning co-processor;

j) initiating a security event upon the receipt of unfavorable results from the scanning co-processor including a situation where malicious code is detected; and

k) processing the data utilizing the central processing unit upon the receipt of favorable results from the scanning co-processor including a situation where malicious code is not detected;

wherein the scanning co-processor is under the control of the central processing unit via the execution of the scanning control logic by the central processing unit;

wherein the criteria is based on a type of a file associated with the data.

35. (Previously Presented) A system for scanning data, comprising:

a) means for executing scanning control logic utilizing a central processing unit;

b) means for identifying a request related to data at the central processing unit;

c) means for determining whether the data meets a predetermined criteria utilizing the central processing unit under the control of the scanning control logic;

d) means for indicating the data to a scanning co-processor coupled to the central processing unit if it is determined that the data meets the predetermined criteria;

e) means for collecting scanning information from memory on the scanning co-processor;

f) means for scanning the data with the scanning co-processor utilizing the scanning information under the control of the scanning control logic;

g) means for waiting for results from the scanning co-processor;

h) means for executing additional logic utilizing the central processing unit while waiting for the results from the scanning co-processor;

i) means for queuing additional data to be scanned by the scanning co-processor while waiting for the results from the scanning co-processor;

j) means for initiating a security event upon the receipt of unfavorable results from the scanning co-processor including a situation where malicious code is detected; and

k) means for processing the data utilizing the central processing unit upon the receipt of favorable results from the scanning co-processor including a situation where malicious code is not detected;

wherein the scanning co-processor is under the control of the central processing unit via the execution of the scanning control logic by the central processing unit;

wherein the criteria is based on a type of a file associated with the data.

36. (Original) The system as recited in claim 35, wherein the scanning information is updated via a network periodically.

37. (Original) The system as recited in claim 35, wherein the additional logic to be executed and the additional data queued to be scanned are handled utilizing multi-threading algorithms.

38. (Previously Presented) The method as recited in claim 1, wherein the criteria is further based on a user.

39. (Previously Presented) The method as recited in claim 1, wherein the criteria is further based on software logic run by a bios.

40. (Previously Presented) The method as recited in claim 1, wherein the scanning control logic is executed automatically.

41. (Previously Presented) The method as recited in claim 1, wherein the scanning control logic is executed automatically when a computer is booted up.

42. (Previously Presented) The method as recited in claim 1, wherein the scanning control logic is executed manually by a user.

43. (Previously Presented) The method as recited in claim 1, wherein the scanning control logic is executed using software logic run by a bios.

44. (Previously Presented) The method as recited in claim 1, wherein the central processing unit aids the scanning co-processor when a large amount of data is to be scanned.

IX EVIDENCE APPENDIX (37 C.F.R. § 41.37(c)(1)(ix))

There is no such evidence.

X RELATED PROCEEDING APPENDIX (37 C.F.R. § 41.37(c)(1)(x))

Since no decision(s) has been rendered in such proceeding(s), no material is included in this Related Proceedings Appendix.

In the event a telephone conversation would expedite the prosecution of this application, the Examiner may reach the undersigned at (408) 971-2573. For payment of any additional fees due in connection with the filing of this paper, the Commissioner is authorized to charge such fees to Deposit Account No. 50-1351 (Order No. NAIIP014/01.128.01).

Respectfully submitted,

By: /KEVINZILKA/ Date: January 3, 2007

Kevin J. Zilka

Reg. No. 41,429

Zilka-Kotab, P.C.
P.O. Box 721120
San Jose, California 95172-1120
Telephone: (408) 971-2573
Facsimile: (408) 971-4660